IN THE CLAIMS

Please amend the claims as follows:

1-18. (Canceled)

19. (Currently Amended) The method of claim ~~18~~ 26, wherein providing a network configuration includes receiving a configuration as the output of a network discovery tool.

20. (Currently Amended) The method of claim ~~18~~ 26, wherein providing a network configuration includes receiving a data file which includes a configuration of the computer network.

21. (Canceled)

22. (Currently Amended) The method of claim ~~21~~ 26, wherein determining vulnerabilities further includes modifying the simulation using a graphical user interface.

23. (Original) The method of claim 22, wherein modifying the simulation includes dynamically interacting with an attacker.

24. (Original) The method of claim 22, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

25. (Original) The method of claim 23, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

26. (Currently Amended) ~~The~~ A method of ~~claim 21~~ analyzing a computer network using a security modeling system, wherein the security modeling system includes a simulator, wherein

the simulator includes a vulnerabilities database of network vulnerability information, the method comprising:

providing a network configuration of a computer network;

simulating the computer network based on the network configuration, wherein simulating the network includes:

receiving mission objectives;

storing the mission objectives; and

simulating the network based on the network configuration and the mission objectives; and

determining vulnerabilities of the computer network using the network vulnerability information stored in the vulnerabilities database, wherein the vulnerabilities database includes an entry for each of a plurality of known network vulnerabilities, wherein each entry includes a service to which the known network vulnerability applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability;

wherein determining vulnerabilities includes computing security results, wherein the security results include a security score.

27. (Currently Amended) The method of claim ~~21~~ 26, wherein determining vulnerabilities of the simulated network further includes updating the vulnerabilities database when vulnerabilities are detected.

28. (Canceled)

29. (Currently Amended) The method of claim ~~28~~ 32, wherein simulating the network further includes receiving commands from a defender and determining results based on the defender commands.

30. (Currently Amended) The method of claim ~~28~~ 32, wherein receiving a network configuration includes receiving critical resource information, wherein the critical resource information includes goals, expectation and constraints for simulating the network.

31. (Currently Amended) The method of claim ~~28~~ 32, ~~and further~~ wherein simulating the network further includes modifying the simulation using a graphical user interface.

32. (Currently Amended) ~~The~~ A method of ~~claim 31~~ opposing network attackers comprising:

receiving a network configuration, wherein the network configuration comprises computer hardware and software component information;

receiving mission objectives including critical resource information used to determine network components that are involved in a specific attack scenario;

receiving commands from a network attacker;

simulating the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components, wherein determining ~~vulnerabilities~~ results includes computing security results which include a security score; and

responding to the network attacker, wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network.

33. (Currently Amended) The method of claim ~~31~~ 32, wherein receiving commands includes receiving attack actions which include commands that simulate service functionality, commands that change services or nodes, and commands that exploit vulnerabilities.

34. (Canceled)

35. (Currently Amended) The system of claim ~~34~~ 37, wherein the mission objectives tables include mission tables, mission files tables and mission services tables.

36. (Currently Amended) The system of claim ~~34~~ 37, wherein the vulnerability tables include service tables.

37. (Currently Amended) ~~The~~ A security modeling system ~~of claim 34~~ for simulating objective networks, comprising:

a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables including information used to determine network components that are involved in a specific attack scenario, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data; and

a graphical user interface which operates with the simulator to allow input and output to clients;

wherein the network configuration tables include configuration tables, defense tables, filter tables, node tables, routing tables and password tables.

38. (Canceled)

39. (Canceled)

40. (Currently Amended) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration, wherein simulating the network includes:

receiving mission objectives;

storing the mission objectives; and

simulating the network based on the network configuration and mission objectives; and

determining vulnerabilities of the simulated network using the vulnerability information stored in ~~the~~ a vulnerabilities database, wherein determining vulnerabilities includes computing security results, wherein the security results include a security score;

wherein the vulnerabilities database includes[:] an entry for each of a plurality of known network vulnerabilities, wherein each ~~network vulnerability~~ entry includes the service to which ~~it~~

the known network vulnerability applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

41. (Canceled)

42. (Currently Amended) The machine-readable medium of claim ~~41~~ 40, wherein mission objectives include critical resource information used to determine network components that are involved in a specific attack scenario.